Learn more about HackerOne

Log in

Program guidelines

Program highlights

Closed Scope
Only accepts reports based on the listed scope.

Fast Payment
Ensures payment within 1 month of receiving a vulnerability report.

Top Response Efficiency
This program's response efficiency is above 90%.

Managed by HackerOne Collaboration Enabled Includes Retesting

10 hours
Average time to first response

1 day, 22 hours
Average time to triage

1 week, 4 days
Average time to bounty

1 week, 6 days
Average time from submission to bounty

2 months, 1 day
Average time to resolution

Rewards summary

Last updated on February 13, 2024. View changes

Each severity lists the 90-day average bounty and the percentage of total resolved reports, if applicable.

Low	Medium	High	Critical
$200	$400–$600	$2,000–$6,000	$12,000–$25,000

Our rewards are based on the severity of a vulnerability. HackerOne uses CVSS 3.0 (Common Vulnerability Scoring Standard) to calculate severity. Please note,

Learn more about HackerOne Log in

each severity level, though bonuses may be given at Amazon's discretion.

SEVERITY	Amount (in USD)
Critical	$12,000 - $25,000
High	$2,000 - $6,000
Medium	$400 - $600
Low	$200
Biz Accepted Risk or Informational	$0

Scope exclusions

Core Ineligible Findings are out of scope. Learn more

Platform standards deviations

This program has not committed to the following Platform Standards. As such the report severity or outcome may differ.

- **Bounty Guidelines for Multiple Reports Highlighting Systemic Issues**
  Amazon rewards for each unique vulnerability defined by single fixes. If there are multiple submissions that impact multiple endpoints but these share a single fix, the first report would be accepted and the following would be considered duplicates.
- **Evaluation and Payment for Bypassing Previously Resolved Vulnerabilities**
  Amazon provides a 25% bypass/incomplete fix bonus on any finding that has been closed for <6 months.

Check here for the full Platform Standards page list.

Overview

Last updated on January 10, 2025. View changes

Learn more about HackerOne Log in

At Amazon, we take security and privacy very seriously. If you believe that you have found a security vulnerability that affects any Amazon product or service, please report it to us. You may report a vulnerability using the “Submit Report” button on this page. Reports that fall within scope of Amazon’s Vulnerability Research Program (VRP) are also eligible for a reward. We appreciate your efforts in helping protect customer trust and make Amazon more secure.

For vulnerabilities related to Amazon Web Services (AWS), please submit reports via the AWS Vulnerability Disclosure Program.
For vulnerabilities related to Amazon Devices, please submit reports via Amazon Vulnerability Research Program - Devices page.
For vulnerabilities related to Ring, please submit reports via the Ring Bug Bounty page
For vulnerabilities related to eero, please submit reports via the eero Bug Bounty page

What is VRP?

VRP is an initiative driven and managed by Amazon's Stores Security Bug Bounty Team.

Who Can Participate in VRP?

Amazon customers and security researchers who discover a potential security finding within Amazon products or services can report it to Amazon's VRP

Amazon employees and contractors, as well as their immediate family members (e.g., parent, sibling, spouse, child) are strictly prohibited from participating in VRP. Amazon employees and contractors may not share information with an external security researcher to bypass this prohibition or otherwise enable another person to participate in VRP (in which case all parties are ineligible). Residents of any countries/regions that are subject to United States sanctions, such as Cuba, Iran, North Korea, Sudan, and Syria or Crimea, and any person designated on the U.S. Department of the Treasury’s Specially Designated Nationals List are strictly prohibited from participating in VRP.

You must be 18 or older to be eligible for an award.

How VRP Works

- Security researchers and Amazon customers are encouraged to report any behavior impacting the information security posture of Amazon products and services.

Learn more about HackerOne Log in

are essential for a quick response.

- We will contact you to confirm that we've received your report and trace your steps to reproduce your research.
- We will work with the affected teams to validate the report.
- We will issue bounty awards for eligible findings. To be eligible for rewards, reports must comply with all parts of this policy and you must be the first to report the issue to us.
- We will notify you of remediation and may reach out for questions or clarification. You must be available to provide additional information if needed by us to reproduce and investigate the report.
- We will work with the affected teams to make necessary improvements and remediation.
- Qualified researchers who regularly submit high quality findings may be added to the **Amazon Private Program** (invited researchers only).

Services and Products in Scope

Bounty eligible findings are limited to following marketplaces and mobile apps: (**Note:** Please check the Scope section for complete details on latest in-scope assets)

All retail marketplaces are Wildcard scoped (*.amazon)

Domain
amazon.com (United States)
amazon.co.uk (UK)
amazon.in (India)
amazon.de (Germany)
amazon.fr (France)
amazon.co.jp (Japan)
amazon.ca (Canada)
amazon.cn (China)
amazon.it (Italy)
amazon.es (Spain)

Learn more about HackerOne Log in

amazon.ae (United Arab Emirates)
amazon.sg (Singapore)
amazon.se (Sweden)
amazon.sa (Saudi Arabia)
amazon.eg (Egypt)
amazon.pl (Poland)
amazon.com.au (Australia)
amazon.com.tr (Turkey)
amazon.com.br (Brazil)
amazon.com.mx (Mexico)
amazon.com.be (Belgium)
amazon.co.za (South Africa)
amazon.com.ng (Nigeria)
amazon.com.co (Colombia)
amazon.cl (Chile)

- Android and iOS Retail Apps (MShop)
  - Android: com.amazon.mShop.android.shopping
  - iOS: amazon-shopping-297606951

GenAI Details and Assessment Considerations for the above

- For any GenAI submissions please include as much of the following information as you can for your report to be considered. Some won't be applicable due to context:
  - Timestamp
  - IP
  - Consumed Content | Prompt String
  - Utterance information (for voice based GenAI)
  - Security Impact

Learn more about HackerOne Log in

Always out of scope and not reward eligible

- Anything which contains aws in the subdomain
- Anything which is .a2z.
- Anything which ends with *.dev
- Anything which redirects to AWS
- Anything which has these types of text in URLs - test, qa, integ, preprod, gamma, beta, user-aliases, regions (us-east, us-west)
- AWS and AWS customer assets

Security issues discovered in the AWS IP Space (https://ip-ranges.amazonaws.com/ip-ranges.json) are not in scope for VRP. This link is a general guideline and not perfect. As an infrastructure provider, AWS customers operate assets in this space. Discovering and testing against AWS and AWS customer assets is strictly out of scope for VRP and against the AWS AUP (https://aws.amazon.com/aup/).

You are not authorized to test any asset, domain, or IP address outside the scope of VRP. If you become aware of an out-of-scope vulnerability, you may report the security finding for our review. If you are not able to demonstrate an impact on bounty-eligible assets, then that finding may not be eligible for the rewards.

Reports of zero-day vulnerabilities (vulnerabilities that were not previously known to the security community) within in-scope services and products will be eligible for an award at our discretion if the report provides significant insight that assists Amazon's security teams with remediation efforts or has not previously been identified by another researcher on our own vulnerability response program.

Rules of Engagement (Behavior)

- Comply with all provisions of this policy at all times, including those regarding who can participate in VRP.
- Test only in-scope services and products, and only test for eligible vulnerabilities. Do not test out-of-scope assets, and do not test for ineligible vulnerabilities or other out-of-scope issues.
- Do not attempt to conduct post-exploitation: modification or destruction of data, interruption or degradation of Amazon services, and pivoting with access not normally granted.
  - Do the minimum amount of testing necessary to identify and validate the finding. Do not perform additional testing after you have confirmed that a vulnerability exists.

Learn more about HackerOne Log in

work to identify the full severity of an issue on the merits of the content itself.
    - Valid Example: A XSS issue that can be escalated with a separate CSRF issue.
    - Invalid Example: Testing many individual instances of a single issue for the purposes of illustrating severity.
    - Invalid Example: Finding disclosed credentials and using them to pivot.

- If, during your testing, you discover a vulnerability that could allow you to bypass an authentication control and gain access to another account, you should report the vulnerability but not take further action with the other account or its data.
- If the vulnerability or your testing causes a readily visible issue that could alert the public to the vulnerability or your testing, immediately report the issue to us, even if your report is incomplete.
- Do not attempt to perform any attack that that could hinder Amazon in serving customers or carrying out other business functions, including brute-force attacks or denial-of-service attacks.
- Use only your own accounts while testing. Do not compromise or test Amazon accounts that are not your own.
    - If you encounter user information that is not your own in the course of your research, please stop and report this activity to our team so we can investigate. Please report to us what information was accessed and delete the data. Do not save, copy, transfer, or otherwise use this data. Continuing to access another person's data may be regarded as evidence of a lack of good faith.
    - You are not authorized to access, use, or otherwise interact with other people's accounts or data.

- Do not attempt to target Amazon personnel or customers, including by social engineering attacks, phishing attacks or physical attacks.
- Do not perform any testing against assets that directly involve Amazon personnel in communication.
    - This can include support chats, even ones appearing to be automated, or Contact Us areas.

- Do not perform physical attacks again any Amazon facility.
- Do not do anything illegal or unethical. You are responsible for complying with local laws, restrictions, regulations, etc.

Rules of Engagement (Testing)

Learn more about HackerOne Log in

applied and scanners/tools must be configured to not send more than 5 requests per second to any particular service.
    - Use of scanning tools without the User-agent string `amazonvrpresearcher_yourh1username` may result in your account/IP getting blocked by automated protections. It can take time to reinstate these so please make sure to include it.

- When testing, do not attempt to execute instructions that may directly or visibly alert other people to your activity or that may access, modify, or delete other people's accounts or data.
- Create Amazon accounts using a HackerOne email to help us track security research activity. You can create accounts on Amazon by using `yourh1username@wearehackerone.com`.
- While testing, forward the string `amazonvrpresearcher¬¬_yourh1username` anywhere in your User-Agent header. You can create a match and replace proxy rule in Burp by going to Proxy >> Options >> Match and Replace with the following options: **Type:** `Request header` **Match:** `^User-Agent.*$` **Replace:** `User-Agent: amazonvrpresearcheryourh1username`
- Do not use 3rd party sites when testing (for instance, XSS Hunter variants). When doing blind XSS or any testing, only utilize assets that you expressly own and control yourself. This can be done using a home-forked version of the xsshunter-express repo. Our concern in using 3rd party infrastructure, exposure of vulnerability and sensitive data to said 3rd parties. Make sure that all traffic goes through domains only you have control over. **Not using a version hosted yourself, will result in complete forfeiture of any reward.**
- Shodan SSL Cert display, and "General Information" may say `Amazon` but is actually an Amazon Customer using AWS. This cannot be used as evidence to determine if something is owned by Amazon, and should not be used as a launch point for recon.
- When testing a subdomain takeover, do not publish anything on the index page or otherwise attempt to demonstrate the overall impact of the vulnerability. Instead, serve an HTML file on a hidden path containing your HackerOne username in an HTML comment.
- Any cache poisoning related testing should be done by adding cache buster parameters to avoid any direct customer impact.
    - For example, https://domain.com/endpoint?cb=test , in this case `cb` is added as a cache buster to prevent any customer impact.

Violation of the above rules may result in forfeit of bounty eligibility, or further, disqualification from bounty program participation at Amazon's discretion.

Learn more about HackerOne Log in

transactions, suspicious password changes, account changes, or potential fraud please contact Customer Service.
- For Amazon Web Services (AWS) related issues, please report via click here.
- To report Copyright Infringement related issues, please report via click here.

Legal Safe Harbor

Amazon will not bring any legal action against anyone who makes a good faith effort to comply with program policies, or for any accidental or good faith violation of this policy.

As long as you comply with this policy:

- We consider your security research to be "authorized" and lawful under the U.S. Computer Fraud and Abuse Act (CFAA), U.S. Digital Millennium Copyright Act (DMCA), and similar laws in the United States and other jurisdictions. This limited authorization does not provide you with authorization to access company data or another person's account.
- We waive any restrictions in our applicable Terms of Service and Acceptable Use Policy that would prohibit your participation in this program in accordance with the terms of, for the limited purpose of your security research under this policy.
- If legal action is initiated by a third party against you in connection with activities conducted under this policy, we will take steps to make it known that your actions were conducted in compliance with this policy.

Amazon cannot authorize any activity on third-party products or guarantee that those third parties won't pursue legal action against you. Amazon is not responsible for your liability from actions performed on third parties.

To protect your privacy, we will not, unless served with legal process or to address a violation of this policy:

- Share your PII with third parties
- Share your HackerOne points, or participation without your permission

If Your Account is Banned or Blocked by Vulnerability Research Activities

- Follow on-screen instructions when you log in into your Amazon account for recovery.
- Be prepared with a recent card statement available to prove ownership.

Research Guidance

Reference HackerOne guidance on writing quality reports:

Learn more about HackerOne Log in

Responsible Disclosure Policy

Thank you for joining us in supporting ethical and responsible disclosure. By participating in this program, you agree not to share publicly or privately any details or descriptions of your findings with any third party. You also agree not to attempt to threaten or extort Amazon.

Amazon commits to timely remediation of your findings, and prompt response to relevant questions.

Severity Examples

	Vulnerability	Severity Range
1	Remote Code Execution	Critical
2	SQL Injection	High - Critical
3	XXE	High - Critical
4	XSS	High - Critical
5	Server-Side Request Forgery	Medium - Critical
6	Directory Traversal - Local File Inclusion	Medium - High
7	Authentication/Authorization Bypass (Broken Access Control)	Medium - High
8	Privilege Escalation	Medium - High
9	Insecure Direct Object Reference	Medium - High
10	Misconfiguration	Low - High
11	Web Cache Deception	Low - Medium
12	CORS Misconfiguration	Low - Medium
13	CRLF Injection	Low - Medium
14	Cross Site Request Forgery	Low - Medium
15	Open Redirect	Low - Medium
16	Information Disclosure	Low - Medium

Learn more about HackerOne Log in

18	Mixed Content	Low

Please note, this is not meant to be an exhaustive list, but a general guideline for what severity these issues are given.

LLM/GenAI Vulnerabilities

Potential Vulnerabilities	Severity	Comments
Unauthorized access/disclosure of PII/PHI data	High-Critical	Severity will be dependent on the context and data classification.
Cross customer sensitive data access	High-Critical	Severity will be dependent on the context and data classification.
Unauthorized system or environment changes	High-Critical	Severity will be dependent on the context and data classification.
Model Theft and LLM training data poisoning	High-Critical	Depending on the overall impact and application context.
Advarsaries can retrieve personal customer data without consent	High-Critical	Severity will be dependent on the context and data classification.
Information Disclosure	Low-Critical	Severity will be dependent on the context and data classification.
Prompt Injection	Medium - Critical	Severity will be dependent on the context and data classification.
Insecure Output Handling	Medium-Critical	Impact will depend on resulting potential vulnerabilities like HTML injection,XSS,SSRF, RCE etc.
Insecure plugins impacting models	Medium-High	Depending on the impact like content injection, code execution, differential error responses, system data exfiltration,
Excessive functionality, permissions and autonomy	Low-High	Depending on the actions allowed by excessive agency issues

Learn more about HackerOne Log in

providing guidance to customers	Medium-High	Severity will be dependent on the context and the guidance.
Adversaries can perform unauthorized actions on behalf of users	Medium-Critical	Depending on the impact, ease and issue radius.
LLM vulnerable to solicitation and social engineering	Medium-High	Depending on the overall impact and application context.
In context data could be used to de-ananoymize users	Medium	Severity will be dependent on the context and data classification.
Absent customer API or data opt out mechanisms	Medium	Severity will be dependent on the context and data classification.
Command Injection	High-Critical	Depending on the impact, ease and issue radius.
API Auth Bypass	High-Critical	Depending on the impact, ease and issue radius.
Runtime Information Disclosure	Low-Medium	Severity will be dependent on the context and data classification.

Non-eligible Vulnerabilities

	Vulnerability
1	Subdomain Takeover for out of scope items or not listed scope. Subdomain Takeovers on Wildcard domains are **In-Scope**
2	Clickjacking
3	Self XSS
4	Email Spoofing - SPF Records Misconfiguration

Out-of-Scope Issues

- Bitflipping, Bitsquatting
- Discovering and testing against AWS customer assets
- Model Hallucinations

Learn more about HackerOne Log in

- Social Engineering, Phishing
- Physical Attacks
- Missing Cookie Flags
- CSRF with minimal impact i.e. Login CSRF, Logout CSRF, etc.
- Content Spoofing
- Stack Traces, Path Disclosure, Directory Listings
- SSL/TLS controls where other mitigating controls exist
- Banner Grabbing
- CSV Injection
- Reflected File Download
- Reports on Out of dated browsers
- Reports on outdated version/builds of in-scope Mobile Apps
- DOS/DDOS
- Host header Injection without a demonstrable impact
- Scanner Outputs
- Vulnerabilities on Third-Party Products
- Auth User Enumeration
- Password Complexity
- HTTP Trace Method

Out-of-Scope Assets

Category	Asset
AWS	All AWS related services and products will be out-of-scope - See AWS security reporting at https://aws.amazon.com/security/vulnerability-reporting/

Top hackers

See all hackers

1 h0nith12 Reputation: 1k

2 itz_mg Reputation: 1k

3 proper-lay Reputation: 682

4 mrxhunt Reputation: 680

5 haxor31337 Reputation: 643

6 m0chan Reputation: 634

Learn more about HackerOne

Log in

9		amalyoman Reputation: 532	10		the_predator Reputation: 511
11		ayush1098 Reputation: 484	12		arielrachamim Reputation: 470

Opportunities
Leaderboard
Status
Support
Press
Terms

Security
Blog
Docs
Disclosure Guidelines
Privacy

© HackerOne